BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 09 456 A 1**

(51) Int. Cl.[7]: **G 06 F 12/14**
G 06 F 3/033

(21) Aktenzeichen: 100 09 456.2
(22) Anmeldetag: 29. 2. 2000
(43) Offenlegungstag: 6. 9. 2001

(71) Anmelder:
Finn, David, 87629 Füssen, DE; Rietzler, Manfred, 87616 Marktoberdorf, DE

(74) Vertreter:
Patentanwälte Böck + Tappe Kollegen, 97074 Würzburg

(72) Erfinder:
gleich Anmelder

(56) Entgegenhaltungen:
DE 197 49 090 A1
DE 197 06 494 A1
DE 296 01 311 U1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Transpondermaus

(57) Sicherheitszugangsverfahren zur Benutzererkennung und/oder Benutzerauthentifikation bei Computervorrichtungen, wobei die Datenübermittlung zwischen einem als Transpondereinrichtung ausgeführten datentragenden Medium und einer Transponderleseeinrichtung erfolgt.

DE 100 09 456 A 1

DE 100 09 456 A 1

Beschreibung

Die Erfindung betrifft ein Sicherheitszugangsverfahren zur verbesserten Benutzererkennung bzw. Benutzerauthentifikation bei Computerarbeitsplätzen. Weiterhin betrifft die Erfindung eine Vorrichtung zur vorteilhaften Durchführung des Sicherheitsverfahrens.

Heutzutage werden auf Computern häufig sicherheitsrelevante Daten gespeichert und bearbeitet. Liegen solche sicherheitsrelevanten Daten vor, so ist der Einblick in diese Daten bzw. deren Weiterverarbeitung auf einen dazu befugten Personenkreis zu beschränken. Eine Möglichkeit, eine solche Beschränkung durchzuführen ist es, die entsprechenden Computersysteme in abgeschlossenen Räumen vorzusehen, zu denen nur der befugte Personenkreis Zugang hat.

In der Praxis ist dieses Vorgehen jedoch oft nicht möglich oder zumindest zeitraubend und umständlich. Vielmehr ist es wünschenswert, daß unterschiedliche Personen einen einzigen Computer benutzen können, ohne daß jeder Zugriff auf alle Daten hat, bzw. daß ein einzelner Benutzer an unterschiedlichen Computern auf die von ihm gewünschten Daten über entsprechend vernetzte Computer zugreifen kann.

Das Vorsehen solcher Möglichkeiten macht es jedoch erforderlich, daß der jeweilige Benutzer am Computer eindeutig und zweifelsfrei identifiziert wird.

Das verbreitetste Verfahren hierzu besteht darin, daß der Benutzer seine Identität in Form einer Benutzerkennung, sowie seine Authentifikation in Form eines Paßwortes beim erstmaligen Zugriff auf den Computer (Einloggen) angibt. Dieses Verfahren weist jedoch etliche Nachteile auf, die die Datensicherheit bei Anwendung dieses Verfahrens beeinträchtigen. So können die Paßwörter nicht allzu lang gewählt werden, da sie sich der Benutzer ansonsten nicht merken kann und aufschreibt, wodurch nicht berechtigte Benutzer den Zugriff auf das Paßwort erlangen können. Kurze Paßwörter können wiederum durch systematisches Ausprobieren gefunden werden. Oft werden auch Paßwörter durch den Benutzer so gewählt, daß diese einfach zu erraten sind, beispielsweise wenn der Benutzer sein Geburtsdatum als Paßwort wählt. Manche Benutzer geben ihr Passwort auch im Freundeskreis weiter, wodurch insbesondere die Vertraulichkeit geheimer Daten gefährdet wird. Eine weitere Sicherheitslücke besteht darin, daß der Benutzer den Arbeitsplatz verläßt, ohne die Sitzung zu beenden (also ohne sich auszuloggen), wodurch ebenfalls unberechtigte Personen Zugriff auf vertrauliche Daten erhalten können. Eine regelmäßige Abfrage der Benutzerkennung und des Paßwortes würde die Sicherheit zwar erhöhen, ist aber nachteilig, da sie den Arbeitsfluß des Benutzers durch regelmäßige Unterbrechungen stören würde.

Um die Probleme des paßwortgeschützten Zugangsverfahrens zu lösen, sind Zugangsverfahren bekannt, bei denen biologische Eigenheiten des jeweiligen Benutzers überprüft werden. So wurden beispielsweise Verfahren zur Spracherkennung, Überprüfung der Unterschrift, Fingerabdruckscanner, Überprüfung der Handkontur, Gesichtserkennung oder Ablesen der Netzhaut des Auges vorgeschlagen. Allen diesen Verfahren ist gemeinsam, daß sie relativ aufwendig sind und somit sinnvollerweise nur am Anfang der Computersitzung (beim Einloggen) abgefragt werden, um so den Arbeitsfluß des Benutzers nicht zu stören. Darüber hinaus sind manche der beschriebenen Verfahren nicht vor Manipulationen sicher, lassen also den Zugang nicht berechtigter Personen zu. Teilweise werden auch berechtigte Benutzer von der Benutzung ausgeschlossen.

Der Erfindung liegt die Aufgabe zugrunde, ein Sicherheitszugangsverfahren vorzuschlagen, das nicht nur den Benutzer eindeutig erkennt, sondern auch dazu geeignet ist,

eine Überprüfung vorzunehmen, ob sich der Benutzer noch am Computer befindet, ohne diesen in seinem Arbeitsfluß zu stören. Ferner liegt der Erfindung die Aufgabe zugrunde, eine Vorrichtung vorzuschlagen, mit der das Sicherheitszugangsverfahren besonders vorteilhaft durchgeführt werden kann.

Diese Aufgabe wird durch ein Verfahren mit den Merkmalen des Anspruchs 1 gelöst. Dabei werden die zur Benutzererkennung bzw. Benutzerauthentifikation zu übermittelnden Daten mittels einer Transponderleseeinrichtung von einem als Transpondereinrichtung ausgeführten datentragenden Medium ausgelesen. Dabei kann entweder nur die Benutzerkennung bzw. nur das Paßwort durch die Transpondereinrichtung übermittelt werden, während die übrigen Eingaben beispielsweise per Tastatur erfolgen. Andererseits können auch sämtliche zur eindeutigen Benutzeridentifikation erforderlichen Daten mittels der Transpondereinrichtung übertragen werden, so daß keine zusätzliche Dateneingabe mehr erforderlich ist. Selbstverständlich kann das erfindungsgemäße Verfahren auch beliebig mit anderen Sicherheitszugangsverfahren wie beispielsweise mit einem Fingerabdruckscanner oder ähnlichen kombiniert werden, um so eine zusätzliche Sicherheitsfunktion zu schaffen. In jedem Fall ermöglicht das erfindungsgemäße Verfahren die eindeutige Identifikation bzw. Authentifikation des Benutzers, ohne daß eine irrtümliche Abweisung des Benutzers, wie sie insbesondere bei biometrischen Verfahren vorkommen können, auftreten. Durch das Speichern der erforderlichen Daten auf einem datentragenden Medium sind auch sehr lange Benutzerkennungen bzw. Passwörter verwendbar, ohne daß das Gedächtnis des Benutzers belastet wird. Durch die Speicherung der Daten auf einem datentragenden Medium wird darüber hinaus die Weitergabe der Benutzerinformationen deutlich erschwert, unabhängig davon, ob diese mit oder ohne Wissen des berechtigten Benutzers geschieht.

Da die Benutzerkennung und -authentifikation auch ohne Mitwirkung des Benutzers geschehen kann, ist eine wiederholte oder auch dauernde Überprüfung möglich, ohne daß der Benutzer in seinem Arbeitsfluß gestört wird.

Es erweist sich als vorteilhaft, wenn sich die Transponderleseeinrichtung in einer Peripherieeinrichtung des Computers befindet, wobei die Peripherieeinrichtung vorzugsweise in unmittelbarerer Nähe des Benutzers vorgesehen ist. Dadurch wird es einfacher, auch bei mehreren unmittelbar nebeneinander angeordneten Computerarbeitsplätzen eine eindeutige Erkennung des vor dem jeweiligen Computerarbeitsplatz befindlichen Benutzers zu erzielen. Darüber hinaus kann mit geringeren Sendeleistungen der Transpondereinrichtung gearbeitet werden, was einerseits ein unberechtigtes Abhören der übermittelten Daten erschwert, andererseits aber auch Vorteile gesundheitlicher Art mit sich bringen kann. So wird beispielsweise die Wahrscheinlichkeit von Herzschrittmacherstörungen oder ähnlichem reduziert, indem die Belastung durch Elektrosmog reduziert wird.

Als besonders vorteilhaft erweist es sich, wenn die Datgen durch eine eine Transponderleseeinrichtung aufweisende Mauseinrichtung ausgelesen werden. Eine Computermaus stellt ein regelmäßig benutztes Eingabegerät dar, so daß sich die Maus fast immer in unmittelbarer Nähe des Benutzers und damit in der Regel der Transpondereinrichtung befindet. Als Mauseinrichtung sind in diesem Zusammenhang selbstverständlich nicht nur Computermäuse sondern auch funktionsähnliche Eingabegeräte wie Touchpads oder Trackballs zu verstehen.

Eine andere bevorzugte Ausführungsform des Zugangsverfahrens besteht darin, daß die Daten mittels einer in einer Tastatureinrichtung eingebauten Transponderleseeinrich-

tung ausgelesen werden. Auch eine Tastatur stellt ein regelmäßig benutztes Eingabegerät dar und befindet sich damit, ebenso wie eine Computermaus, normalerweise in unmittelbarer Nähe des Benutzers. Auch hier ist unter einer Tastatureinrichtung nicht nur eine Computertastatur an sich, sondern auch Kombigeräte, wie beispielsweise Touchpads aufweisende Tastaturen und ähnliches zu verstehen.

Besonders vorteilhaft ist es, wenn das datentragende Medium zur Datenübermittlung in eine Ausnehmung einer Halteeinrichtung eingeführt wird, wobei die Halteeinrichtung sich in einer Peripherieeinrichtung oder in deren unmittelbarer Nähe befinden kann. Durch diese Anordnung befindet sich die Transpondereinrichtung einerseits näher an der Transponderleseeinrichtung, andererseits weiter vom Benutzer entfernt, so daß mit einer weiter verringerten Sendeleistung gearbeitet werden kann. Die eindeutige Zuordnung des Benutzers zur Computereinrichtung wird gefördert. Schließlich wird auch das Verständnis des Benutzers, ob er gerade eingeloggt ist oder nicht, gefördert: Bei einer entsprechenden Ausführung, insbesondere der Sendeleistung, wird der Benutzer nur dann identifiziert, wenn sich das datentragende Medium in der Ausnehmung befindet, und wird entsprechend nicht identifiziert, wenn er das datentragende Medium aus der Halteeinrichtung entfernt. Die beschriebenen Halteeinrichtungen können vorteilhafterweise in einer Tastatur, in einer Computermaus, in einem Mauspad oder im Monitor vorgesehen werden.

Eine vorteilhafte Weiterbildung des Verfahrens erhält man, wenn die von der Transpondereinrichtung gesendeten Daten von einer insbesondere in der Halteeinrichtung vorgesehenen Verstärkungseinrichtung verstärkt werden. Dadurch kann die Qualität der Datenübertragung verbessert werden, so daß Übermittlungsfehler verringert werden. Trotzdem kann das datentragende Medium weiterhin sehr kompakt ausgeführt werden, weil die darin vorgesehene Transpondereinrichtung selbst keine große Sendeleistung aufweisen muß. Weiterhin kann die Verstärkereinrichtung auch mit Batterien oder einer externen Stromversorgung versehen werden, so daß eine erhöhte Sendeleistung vorgesehen werden kann, ohne daß eine Stromversorgung der im datentragenden Medium vorgesehenen Transpondereinrichtung nötig wäre.

Als besonders vorteilhaft erweist es sich, wenn die Datenübermittlung insbesondere zwischen Transpondereinrichtung und Transponderleseeinrichtung in kryptographisch verschlüsselter Form erfolgt. Dadurch wird ein unbefugtes Mitlesen der zwischen Transpondereinrichtung und Transponderleseeinrichtung übermittelten Daten deutlich erschwert. Ebenso wird es schwieriger, die auf dem datentragenden Medium gespeicherten Daten durch einen unbefugten Lesezugriff zu erlangen. Dabei ist es unerheblich, ob das kryptographische Verfahren auf einem symmetrischen Schlüssel wie beispielsweise dem DES-Algorithmus oder auf einem asymmetrischen Schlüssel, wie bei den RSA- oder Diffie-Hellmann-Verfahren beruht. Vorzugsweise wird kein fester Schlüssel verwendet, sondern ein Schlüssel, der zumindest in regelmäßigen Abständen neu vereinbart wird.

Eine vorteilhafte Weiterbildung des Sicherheitszugangsverfahrens weist die Eigenschaft auf, daß die Datenübermittlung permanent bzw. in periodischen Intervallen erfolgt. Durch die ständige bzw. periodische Abfrage der Benutzerdaten kann überprüft werden, ob sich der Benutzer noch vor dem Computer befindet oder ob er zwischenzeitlich den Arbeitsplatz verlassen hat. Eine erhöhte Sicherheit wird dadurch gefördert. Je häufiger die Datenübermittlung erfolgt, desto kürzer ist die Zeit, in der der Computer noch Eingaben entgegen nimmt, obwohl der Benutzer den Arbeitsplatz bereits verlassen hat, und um so größer ist die Datensicherheit. Es kann sich jedoch als vorteilhaft erweisen, die Zeitspanne zwischen den einzelnen Abfragen relativ lang zu wählen, um den Energieverbrauch, insbesondere bei batteriebetriebenen Vorrichtungen, möglichst gering zu halten und um elektromagnetische Abstrahlungen zu reduzieren.

Eine dazu alternative vorteilhafte Weiterbildung des Verfahrens besteht darin, daß die Daten nur nach Anforderung, insbesondere um sicherheitsrelevante Tätigkeiten zu autorisieren, erfolgt. Dabei ist es beliebig, ob die Anforderung von seiten des Computers oder ob die Anforderung von seiten des Benutzers erfolgt. Beispielsweise kann die Datenübermittlung beim Einloggen, vor dem Löschen einer Datei oder zur Genehmigung einer Überweisung bei einer Homebanking-Anwendung erfolgen. Dadurch wird die Größe des von der Transpondereinrichtung abgestrahlten Datenvolumens deutlich verringert, andererseits ist der Schutz bei sicherheitsrelevanten Tätigkeiten nach wie vor sehr hoch.

Besonders vorzugsweise wird die Datenübermittlung durch den Benutzer, beispielsweise durch einen Druck auf eine Datenübermittlungstaste ausgelöst. Dadurch kann der Benutzer besonders sicherheitsrelevante Operationen nochmals bestätigen oder abbrechen, bevor diese ausgeführt werden.

Als besonders vorteilhaft erweist es sich für das Verfahren, wenn die Daten aus einer in Gebrauchsgegenständen integrierten Transpondereinrichtung ausgelesen werden, bzw. wenn die Transpondereinrichtung als Gebrauchsgegenstand ausgeformt ist. Beispielsweise könnte der Transponder in Form eines Fingerrings ausgeführt sein. In einem solchen Fall könnte der Transponder praktisch nicht mehr vor dem Computer vergessen werden und würde zusätzlich in der Regel vom Benutzer mitgeführt werden, wenn er auf einem Computer zuzugreifen beabsichtigt. Eine besonders hohe Sicherheit wird dadurch gefördert. Statt eines Fingerrings könnten insbesondere auch Uhren, Namensschilder und ähnliches Anwendung finden.

Eine vorteilhafte Vorrichtung zur Durchführung des erfindungsgemäßen Verfahrens weist eine mit einer Computereinrichtung zusammenwirkende Transponderleseeinrichtung sowie ein als Transpondereinrichtung ausgeführtes datentragendes Medium auf. Somit weisen die Vorrichtungen, die oben im Zusammenhang mit dem Verfahren beschriebenen Vorteile ebenfalls auf.

Vorteilhafte Weiterbildungen der Erfindung ergeben sich aus den Unteransprüchen.

Im folgenden ist zur Verdeutlichung der Erfindung ein Ausführungsbeispiel unter Bezugnahme auf die dargestellten Figuren beschrieben. Dabei wird insbesondere bei der Darstellung der Computermaus, ein IBM®-kompatibler Computer zugrunde gelegt. Die Erfindung läßt sich jedoch ohne Einschränkungen auch mit Computern beliebiger Hersteller mit beliebigen Betriebssystemen realisieren.

Es zeigen:

Fig. 1 eine Computermaus mit einer Transponderleseeinrichtung in Draufsicht;

Fig. 2 ein Mauspad mit einer Verstärkereinrichtung und einer Ausnehmung zur Aufnahme einer kartenförmigen Transpondereinrichtung in Draufsicht;

Fig. 3 ein kartenförmig ausgeformtes datentragendes Medium mit einer Transpondereinrichtung in Draufsicht;

Fig. 4 ein als Fingerring ausgeformtes datentragendes Medium mit einer Transpondereinrichtung im Querschnitt von der Seite aus gesehen.

In **Fig.** 1 ist eine Computermaus **10** dargestellt, in welcher eine Transponderleseeinrichtung **20** eingebaut ist. Die Maus ist über ein Kabel **11** mit einem hier nicht dargestellten Computer verbunden und wird einerseits über das Kabel **11** mit Strom versorgt, andererseits sendet sie über das Kabel

11 die Information über Mausbewegungen, Tastendrücke und von der Transpondereinrichtung empfangene Daten.

Die Transponderleseeinrichtung **20** besteht im wesentlichen aus einer Lesespule **21** sowie einer Leseelektronik **22**. Dabei kann die Lesespule **21** in an sich bekannter Weise so ausgeführt sein, daß diese die Energie an eine sogenannte passive Transpondereinheit übermittelt, so daß die passive Transpondereinheit keine eigene Energieversorgung, wie beispielsweise Batterien, benötigt. Die von der Lesespule **21** empfangenen Daten werden von der Leseelektronik **22** aufbereitet und anschließend über das Kabel **11** an ein entsprechend ausgeführtes, hier nicht näher dargestelltes Treiberprogramm des Computers übermittelt, der die Daten der Transponderleseeinrichtung **20** an die entsprechenden Anwendungsprogramme bzw. das Betriebssystem weiterleitet.

Die dargestellte Computermaus **10** weist, wie bei Computermäusen für IBM®-kompatible Computer üblich, zwei Maustasten **30** und **31** auf. Die Erfindung ist jedoch auch für dreitastige Computermäuse, die mit dem Betriebssystem UNIX zusammenarbeiten, bzw. für eintastige Computermäuse für Computer der Firma Apple® anwendbar. Selbstverständlich können auch Sonderfunktionen aufweisende Mäuse, wie z. B. Radmäuse der Firma Logitec® für die Benutzung der vorliegenden Erfindung ensprechend angepaßt werden. Zusätzlich zu normalen Computermäusen, gleich welchen Typs, verfügt die dargestellte Computermaus **10** über eine zusätzliche Datenübermittlungstaste **32**.

Sollen auf dem Computer bestimmte, insbesondere sicherheitsrelevante Operationen durchgeführt werden, wie beispielsweise das Einloggen, das Löschen von Dateien, oder die Ausführung einer Überweisung bei Homebanking-Anwendungen, so fordert das entsprechende Anwendungsprogramm die entsprechenden Benutzerdaten über die Transponderleseeinrichtung **20** der Computermaus **10** von einer Transpondereinrichtung **210** (**Fig.** 3), 310 (**Fig.** 4) eines datentragenden Mediums **200** (**Fig.** 3), 300 (**Fig.** 4) an. Diese Abfrage wird jedoch zunächst nicht durchgeführt, sondern es erfolgt beispielsweise eine Bildschirmmeldung für den Benutzer, daß dieser die entsprechende Operation genehmigen soll. Ist der Benutzer mit der Operation einverstanden, so drückt er die Datenübermittlungstaste **32** so daß die Benutzerdaten übermittelt werden und die Operation durchgeführt wird. Ansonsten kann er die Durchführung der Operation durch einen beliebigen, anderen Tastendruck unterbinden. Somit wird eine zusätzliche Sicherheit schutzbedürftiger Daten bzw. bei sicherheitsrelevanten Operationen gefördert.

In **Fig.** 2 ist ein Mauspad **100** zur vorteilhaften Zusammenarbeit mit einer Computermaus **10** nach **Fig.** 1 in Draufsicht dargestellt. Das dargestellte Mauspad weist eine Halteeinrichtung **110** mit einer Ausnehmung **111** auf, in das das hier kartenförmig ausgeformte datentragende Medium **200** nach **Fig.** 3 eingeführt werden kann. Wird das datentragende Medium **200** in die Ausnehmung **111** eingeführt, so koppelt eine Sendespule **211** der Transpondereinrichtung **210** an eine Empfangsspule **115** des Mauspads an und kann so mit geringster Sendeleistung Daten übertragen. Die von der Empfangsspule **115** empfangenen Daten werden über eine Verstärkereinrichtung **116** verstärkt und anschließend von einer Rahmenspule **117** mit vorzugsweise höherer Sendeleistung abgestrahlt und anschließend von der Transponderleseeinrichtung **20** der Computermaus **10** empfangen. Vorzugsweise setzt eine Verstärkereinrichtung **116** zusätzlich die Frequenz der übermittelten Daten um, so daß eine Rückkopplung zwischen Empfangsspule **115** und Rahmenspule **117** vermieden wird.

In **Fig.** 3 ist das kartenförmig ausgeführte datentragende Medium **200**, welches vorteilhaft in die entsprechend ausgeführte Ausnehmung **111** des in **Fig.** 2 dargestellten Mauspads **100** eingeführt werden kann, dargestellt. Das datentragende Medium **200** besteht in an sich bekannter Weise aus einem Kartenkörper **201**, in dem sich eine Transpondereinrichtung **210** befindet. Die Transpondereinrichtung besteht, wie üblich, aus einer Sendespule **211** und einer Transponderelektronik **212**. Für die Erfindung ist es unerheblich, wie die Transpondereinrichtung **210** im Detail ausgeführt ist. Beispielsweise kann es sich bei der Sendespule **211** um eine Verlegespule oder Wickelspule handeln. Die Transponderelektronik **212** kann einteilig oder mehrteilig ausgeführt sein. Darüber hinaus kann die Transponderelektronik **212** auch auf Funktionen eines kryptographischen Coprozessors zugreifen, um eine kryptographische Verschlüsselung der zu übermittelnden Daten zu beschleunigen.

In **Fig.** 4 ist eine alternative Ausführungsform der Transpondereinrichtung dargestellt. Hierbei handelt es sich um das als Fingerring ausgeformte datentragende Medium **300**. Die Transpondereinrichtung **310** ist bei dieser Ausführungsweise vom Basismaterial des Fingerrings **301** aufgenommen, und besteht, analog zu **Fig.** 3 aus einer Sendespule **311** und einer Transponderelektronik **312**. Besonders vorteilhaft ist bei dieser Ausführungsweise, daß das datentragende Medium **300** an den Finger gesteckt werden kann und somit, ohne den Benutzer zu behindern, vom Benutzer ständig mitgeführt werden kann, und insbesondere auch nicht vom Benutzer beim Verlassen des Arbeitsplatzes dort vergessen werden kann. Weiterhin ist bei dieser Ausführungsweise vorteilhaft, daß das datentragende Medium an der Hand des Benutzers steckt, und sich somit üblicherweise in der Nähe der Computermaus **10** oder der Tastatur des Computers befindet, so daß für die Datenübermittlung keine große Wegstrecke zu überbrücken ist. Die Sendeleistung kann somit entsprechend klein gewählt werden.

Patentansprüche

1. Sicherheitszugangsverfahren zur Benutzererkennung und/oder Benutzerauthentifikation bei Computervorrichtungen, **dadurch gekennzeichnet**, daß die Datenübermittlung zwischen einem als Transpondereinrichtung (**210**, **310**) ausgeführten datentragenden Medium (**200**, **300**) und einer Transponderleseeinrichtung (**20**) erfolgt.
2. Sicherheitszugangsverfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Daten durch eine eine Transponderleseeinrichtung (**20**) aufweisende Peripherieeinrichtung (**10**) ausgelesen werden.
3. Sicherheitszugangsverfahren nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, daß die Daten durch eine eine Transponderleseeinrichtung (**20**) aufweisende Mauseinrichtung (**10**) ausgelesen werden.
4. Sicherheitszugangsverfahren nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, daß die Daten durch eine eine Transponderleseeinrichtung (**20**) aufweisende Tastatureinrichtung ausgelesen werden.
5. Sicherheitszugangsverfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß für die Datenübermittlung das datentragendes Medium (**200**, **300**) in eine Ausnehmung (**111**) einer Halteeinrichtung (**110**), welche sich insbesondere in der Peripherieeinrichtung (**10**) oder deren unmittelbarer Nähe befindet, eingeführt wird.
6. Sicherheitszugangsverfahren nach einem der vorangehenden Ansprüche, insbesondere nach Anspruch 5, dadurch gekennzeichnet, daß die Signale der Transpondereinrichtung (**210**, **310**) von einer Verstärkungseinrichtung (**116**) verstärkt werden.

7. Sicherheitszugangsverfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß die Datenübermittlung in kryptographisch verschlüsselter Form erfolgt.

8. Sicherheitszugangsverfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß die Datenübermittlung permanent bzw. in periodischen Intervallen erfolgt.

9. Sicherheitszugangsverfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß die Datenübermittlung nur nach Anforderung, insbesondere zur Genehmigung sicherheitrelevanter Tätigkeiten, erfolgt.

10. Sicherheitszugangsverfahren nach einem der vorangehenden Ansprüche, insbesondere nach Anspruch 9, dadurch gekennzeichnet, daß die Datenübermittlung durch den Benutzer, insbesondere durch einen Druck auf eine Datenübermittlungstaste (**32**), ausgelöst wird.

11. Sicherheitszugangsverfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß die Daten aus einem in Gebrauchsgegenständen (**301**) integrierten datentragenden Medium (**200, 300**) bzw. einem als Gebrauchsgegenstand (**301**) geformten datentragenden Medium ausgelesen werden.

12. Vorrichtung zur Durchführung des Sicherheitsverfahrens nach einem der Ansprüche 1 bis 11, gekennzeichnet durch, eine mit einer Computereinrichtung zusammenwirkenden Transponderleseeinrichtung, sowie ein als Transpondereinrichtung (**210, 310**) ausgeführtes datentragendes Medium (**200, 300**).

13. Vorrichtung nach Anspruch 12, dadurch gekennzeichnet, daß die Transponderleseeinrichtung (**20**) in eine Peripherieeinrichtung (**10**) eingebaut ist.

14. Vorrichtung nach einem der Ansprüche 12 oder 13, dadurch gekennzeichnet, daß die Transponderleseeinrichtung (**20**) in eine Mauseinrichtung (**10**) eingebaut ist.

15. Vorrichtung nach einem der Ansprüche 12 oder 13, dadurch gekennzeichnet, daß die Transponderleseeinrichtung (**20**) in eine Tastatureinrichtung eingebaut ist.

16. Vorrichtung nach einem der Ansprüche 12 bis 15, dadurch gekennzeichnet, daß eine Halteeinrichtung (**110**), welche insbesondere in der Peripherieeinrichtung (**10**) oder deren unmittelbarer Nähe vorgesehen ist, eine Ausnehmung (**111**) zur Aufnahme des datentragenden Mediums (**200, 300**) aufweist.

17. Vorrichtung nach einem der Ansprüche 12 bis 16, insbesondere nach Anspruch 16, dadurch gekennzeichnet, daß die Halteeinrichtung (**110**) eine Verstärkungseinrichtung (**111**) aufweist, die die übermittelten Daten verstärkt.

18. Vorrichtung nach einem der Ansprüche 12 bis 17, dadurch gekennzeichnet, daß die Transponderleseeinrichtung (**20**) und das datentragende Medium (**200, 300**) ein kryptographisch verschlüsselndes bzw. ein kryptographisch entschlüsselndes Mittel aufweisen.

19. Vorrichtung nach einem der Ansprüche 12 bis 18, dadurch gekennzeichnet, daß die Transponderleseeinrichtung (**20**) und das datentragende Medium (**200, 300**) so ausgeführt sind, daß sie einander permanent bzw. in periodischen Intervallen Daten übermitteln.

20. Vorrichtung nach einem der Ansprüche 12 bis 18, dadurch gekennzeichnet, daß die Transponderleseeinrichtung (**20**) und das datentragende Medium (**200, 300**) so ausgeführt sind, daß sie nur nach Anforderung, insbesondere zur Durchführung sicherheitsrelevanter Tätigkeiten, einander Daten übermitteln.

21. Vorrichtung nach einem der Ansprüche 12 bis 20, insbesondere nach Anspruch 20, dadurch gekennzeichnet, daß die Transponderleseeinrichtung (**20**) und das datentragende Medium (**200, 300**) so ausgeführt sind, daß sie nach Auslösung durch den Benutzer, insbesondere durch den Druck auf eine Datenübermittlungstaste (**32**), einander Daten übermitteln.

22. Vorrichtung nach einem der Ansprüche 12 bis 21, dadurch gekennzeichnet, daß das datentragende Medium (**200, 300**) als Gebrauchsgegenstand (**301**) ausgeformt ist bzw. von einem Gebrauchsgegenstand (**301**) aufgenommen wird.

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 100 09 456 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 6. September 2001

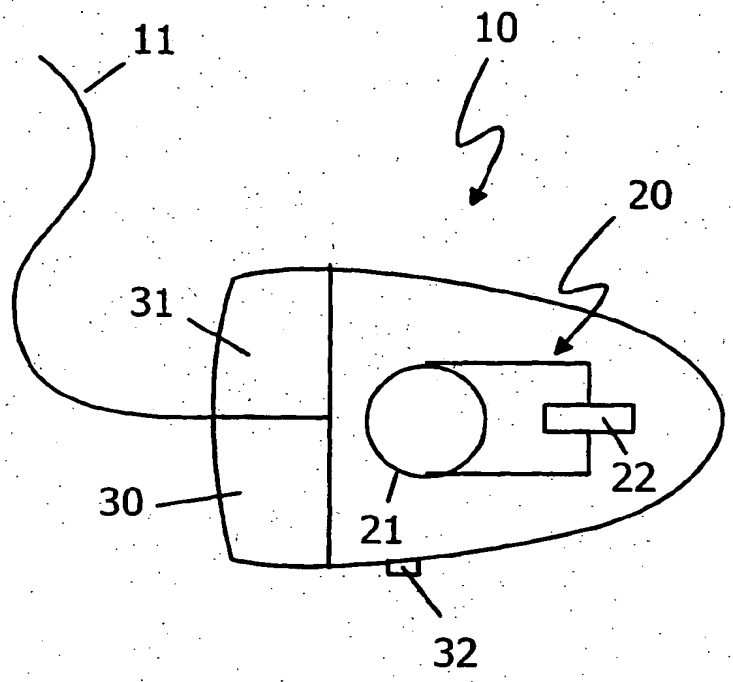

Fig. 1

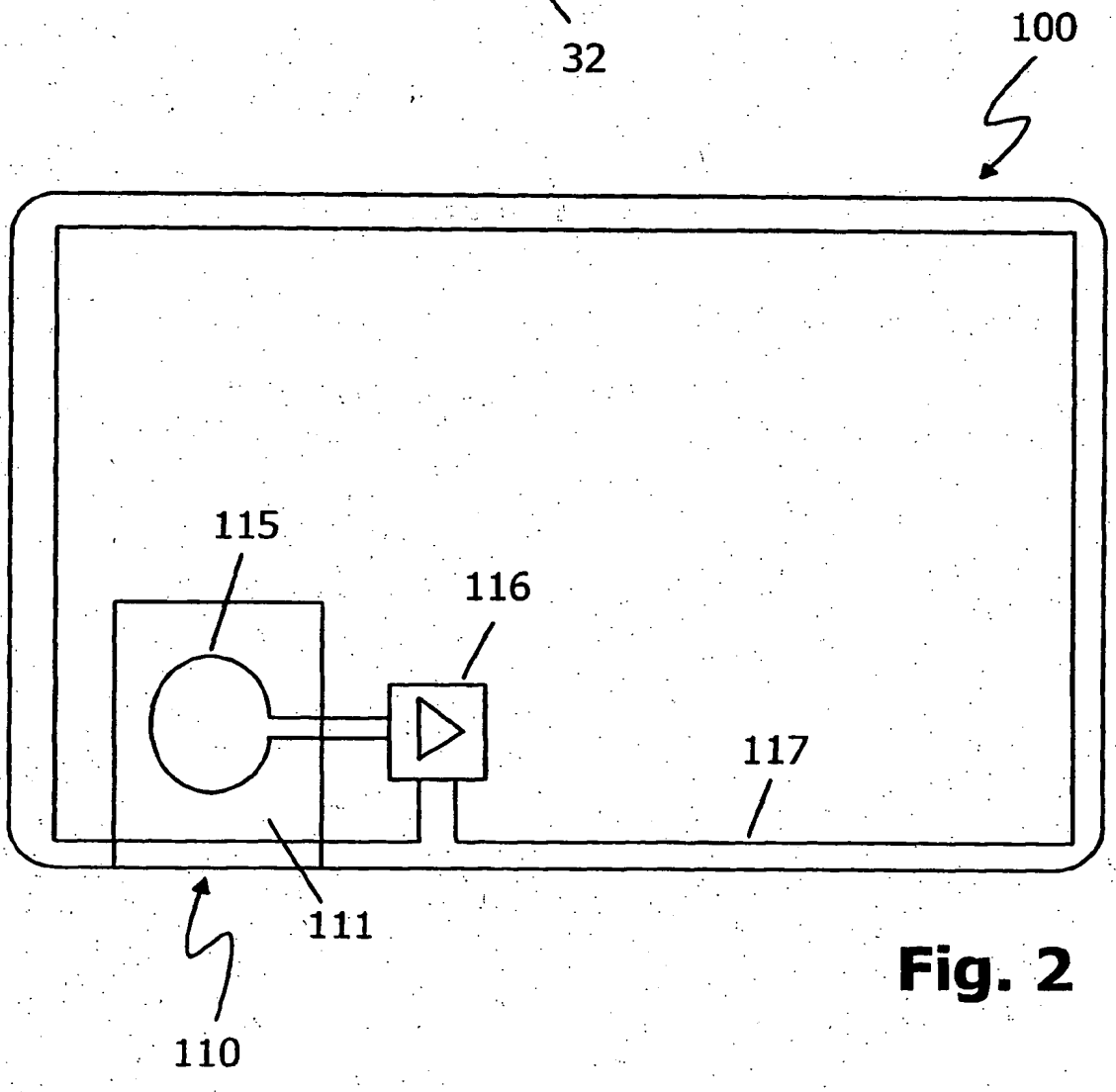

Fig. 2

Nummer: DE 100 09 456 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 6. September 2001

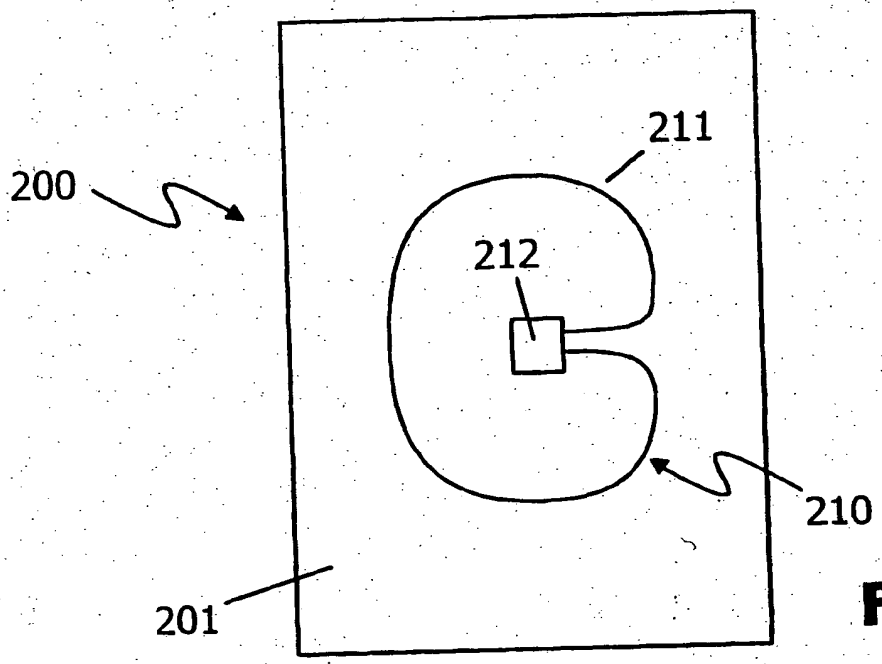

Fig. 3

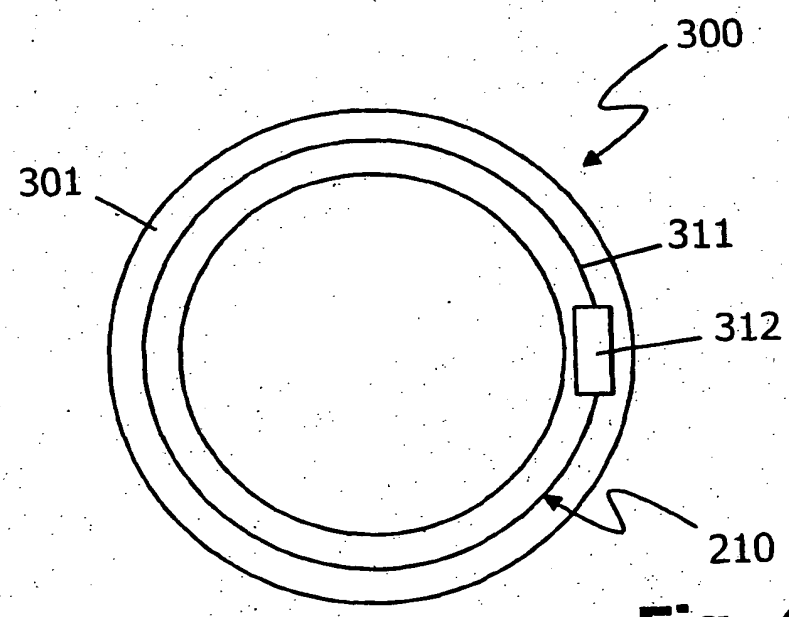

Fig. 4